AU/ACSC/5977/2010-11

COMMANDERS AND CYBER CHAT:

SHOULD MORE GUIDANCE BE PROVIDED FOR SOCIAL NETWORKING SITES?

By

Major Courtney Finkbeiner

A Research Report Submitted to the Faculty

In Partial Fulfillment of Graduation Requirements

Advisors: Major Lynn Schmidt & Major Ryan Oakley

Air Command and Staff College

Maxwell Air Force Base, Alabama

April 2011

Commanders & Cyber Chat
Independent Research

Abstract

Social networking websites have emerged as the new meeting place in the twenty-first century. Cyber chat connects people with shared dialogue, information and pictures in public communities with hundreds of members. Recognizing the significance of this information tool, the Pentagon has allowed all soldiers to utilize social networking sites on the military's non-classified computer networks.[1] Multiple military leaders have even started their own social blogs on Facebook or Twitter to share information and garner feedback from their troops. [2] Risks are inherent to public websites, and a certain amount of privacy is sacrificed in virtual societies. The limited guidance provided by higher headquarters regarding social networking responsibilities is lacking and fails to answer important questions that put the reputation of commanders and supervisors in jeopardy. Will accepting a friend request lead to perceptions of unprofessional relationships between supervisors/subordinates or officers/enlisted? To what extent are local commanders responsible for determining the participation in "groups" or the meaning of context posted by users of their Facebook pages?

Introduction

In response to malicious risks posed by social media, the Department of Defense (DOD) has outlined a new policy, *Directive-Type Memorandum 09-026*, to protect against cyber attacks, safeguard military missions, and maintain adequate bandwidth.[3] Unfortunately, the new DOD policy leaves an abyss of discretion at the hands of local commanders. In particular are the risks of indiscreet information sharing in virtual communities with both supervisors and subordinates, and consequently how that information can be viewed negatively for military members. This paper will outline the background on social network sites and examine the myriad of challenges facing commanders in monitoring/policing virtual communities. In addition, this paper will introduce 2011 survey results from two distinct groups of officers at Maxwell Air Force Base on social networking. The findings from the data include implications for commanders on friending, privacy and guidance on social networks. Finally this paper will propose guidance for military members and commanders regarding management of social network sites.

According to the only Air Force social media survey, which is from 2008, 75% of Airmen use MySpace, 70% use YouTube, and 50% use Facebook. From those results, 42% of E-2's use Facebook and 60% of second lieutenants use Facebook. Additionally, 75% of E-2 to E-5 use MySpace, and 43% of that group uses it several times a day.[4] Two years later, the DOD has made social networking sites available on government computers. With 500,000 new global users per day joining MySpace and Facebook daily, there is undoubtedly an increase in the number of airmen using these sites especially when it can be done on duty.[5] In 2010, The Air Force Public Affairs Department published *Social Media and the Air Force*, to provide guidance to airmen about social networking. The document points out that public opinion and institutional standing are evaluated daily through social media postings made by Airmen, and even if members state they are not representing the Air Force on social networking sites, other audiences may not interpret the information similarly.[6] The interpretation of that information can cause challenges for commanders.

Social Network Background

What is the allure of social networks? D. Boyd (2007) describes the magnetism of social networking in the cyber domain as sites that attract people based on shared interests, political views, shared racial, sexual, religious or nationally-based identities. Social web-based networks are unique because they enable users to articulate and make visible their social connections with friends, family and colleagues. Participants are not looking necessarily for business networking, but rather they are primarily communicating with people who are already part of their extended social network. Social networking sites are primarily organized around people, not interests. They have a personal structure, with the individual at the center of their own community. Boyd points out that Facebook is used to maintain existing off-line relationships or solidify off-line connections.[7] The Defense Department has accepted utilizing social networking sites, as stated by David Wennergren, Deputy Assistant Secretary of Defense for Information Technology, "We need to take advantage of these capabilities that are out there-this Web 2.0 phenomena."[8]

Social networking sites consist of visible profiles with user demographic data such as name, occupation, age, location, or marital status.. Additionally, users can advertise their likes, interests, or group affiliation. After completing the profile page, users can ascertain with whom they have shared interests and invite them to join their social network. To initiate the invitation, the user must send a friend request. After the friend request is accepted, that person appears on the user's profile list of friends.[9] Friends who have permission to view a user's profile also have permission to view links to the user's list of friends, hence interconnecting everyone on the user's profile.[10] Facebook makes individual friend profiles visible to anyone in the group or networks that a user belongs to; even if those individuals are not directly connected or know all of the network members.[11]

Challenges for Commanders

Friending. The distinction between genuine friends and social network acquaintances can become blurred in cyber markets. A research study conducted by Fono & Raynes-Goldie (2006) discovered two dominant perceptions of "friending" in social networks. On one hand, the perception is there should be rules of etiquette for friending someone related to social norms of endorsing that person as a close contact with trust. On the other hand, there is a perception that friending is simply a system descriptor, and this description does not necessarily imply a close relationship. The research continued to illustrate that users who experienced a high degree of social conflict tended to be the same users who reported a greater degree of adherence to the norms relating to friending as a close contact.[12]

An additional complication to online chat is computer mediated communication or typed communication. Typed communication tends to develop inflated or unrealistic concepts of one another due to the absence of verbal, visual and contextual cues that are usually present in face-to-face interactions.[13] Users tend to perceive only fragments of the situation and fill in the blanks with their own assumptions based on the meager information available.[14] Interpretation of these virtual relationships and conversations will prove to be challenging for commanders, and leads to many questions such as: Who should initiate a friend request if the purpose is to simply share information or viewpoints related to an operational concern? Will accepting a friend request lead to perceptions of unprofessional relationships between supervisors/subordinates or officers/enlisted.

Deciphering Content. Commanders have the inherent authority and responsibility to execute the mission, protect resources, and maintain good order and discipline. According to *The Military Commander and the Law,* published by the Judge Advocate Generals School, this authority and responsibility includes placing lawful restrictions upon opposition and protest activities. At the same time, commanders must preserve the service member's right of expression, consistent with good order, discipline and national security, to the maximum extent possible.[15] Military personnel must reject participation in organizations that espouse supremacist causes; attempt to create illegal discrimination based on race, creed, color, sex, religion, or national origin; advocate the use of force or violence; or otherwise engage in an effort to deprive individuals of their civil rights.[16]

"Cybervetting" is a new term used to assess an individual's suitability to hold a position or security clearance using in part information found on the Internet.[17] When it comes to positions of trust such as the DOD or law enforcement, state and local officials are turning to the Internet as a resource for background checks. Thanks to the relative ease of searching and finding data on the web, employers can verify qualifications and eligibility of applicants and identify individuals who compromise their position of trust.[18] One of the drawbacks to searching the Internet for information is how the employer deciphers the content. To date, there are no guidelines for employees to confirm the accuracy of any information found online. *Developing a Cybervetting Strategy for Law Enforcement*, companion study for national security, suggests that applicants and incumbents seeking law enforcement positions may be asked to access password protected websites in order for the background investigator to review the applicant's profile, blogs, or other online forums for disqualifying content.[19] As military members are in positions of public trust, should commander's use information on subordinates social networking sites to verify qualifications or compromise of positions?

What is considered taboo in the public sector is now being seen more on social network sites. For example, a fictitious user TOPDOG puts on his profile his favorite book is *Mein Kampf*, his favorite movie is the Nazi propaganda film, *Triumph of the Will*, his interests are "white women, and his dislikes include anyone who opposes the master race. On Facebook, individuals can join "groups" with similar interests as their own, and similarly individuals can edit their profiles to show their specific interests. Dozens of members of *newsaxon.org*, a white supremacist social network site, have identified themselves proudly as active duty members of the United States armed forces.[20] What if a service member wearing a Navy uniform and holding a Confederate insignia is on a commander's friends list? Is that commander responsible for determining the meaning of his Facebook friends profile pictures? To what extent are local commanders responsible for determining the participation in "groups" or the meaning of context posted by users of their Facebook pages?

Privacy. Network user naivety has attracted the attention of employers. Few people take time to read the small print on user agreements for social networking sites, and what users once thought was a private forum is actually open to monitoring. Facebook's user agreement terms state, "We may collect information about you from other Facebook users. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy setting or security measures on Facebook."[21] To drive home social networking sites inability to protect privacy, here are a few examples of information sharing that resulted in negative outcomes: Twenty-seven workers from the Automobile Club of Southern California were fired for their comments about colleagues on their MySpace accounts; a sheriff was fired for revealing on Facebook his heavy drinking and fascination with female breasts; a Catholic school teacher was fired after posting on Facebook that he was gay; a man absent from work for a family emergency was fired when his Facebook pictures revealed he was actually at a Halloween party in drag.[22] Given these examples, are military commanders, like other employers, now required to police virtual neighborhoods for employees who reveal personal information discrediting their position, title, and rank?

The civilian sector is not the only group receiving negative attention on so-called private social networking sites. Lieutenant General William Caldwell, *Combined Security Transition*

Command-Afghanistan, and his staff have found themselves in the middle of a public firestorm regarding information operations. In an article by Michael Hastings in *Rolling Stone* magazine, Lt. Gen. Caldwell persistently encouraged his officers to use Facebook as part of a "social networking initiative." Lieutenant Colonel Michael Holmes, Lt. Gen. Caldwell's leader of the Information Operations unit, is under investigation for "using Facebook too much." The investigation reveals Lt. Col Holmes made comments about Afghan men wanting to hold his hand and discussed his sexual needs. "Lt. Col Holmes comments about his sexual needs are even more distasteful in light of his status as a married man," concluded the report.[23] The same article describes Facebook comments made by Colonel Gregory Breazile, Lt. Gen. Caldwell's spokesman for the Afghan training mission. Col. Breazile's comments include "multiple references to drinking alcohol and a photo of a warning inside a Port-o-John mocking Afghans--'In case any of you forgot that you are supposed to sit on the toilet and not stand on it and squat. It's a safety issue. We don't want you to fall in or miss your target.'"[24] Given these examples, are military commanders, like other employers, now required to police virtual neighborhoods for employees who reveal personal information discrediting their position, title, and rank?

Professional & Unprofessional Relationships. In 2009, Admiral Mike Mullen, the chairmen of the Joint Chiefs of Staff, acknowledged problems with social networking sites, stating "Sometimes people, because of the nature of these sites, can have a tendency to get lax in what they put on there. We have to educate people that, just like any other types of communications, you have to make sure that you're protecting information that is of operational concern."[25] Mullen has his own Facebook page where he has 16,500 following his posts. His Facebook page is open to the public and anyone can read his posts; however, Mullen's page is not open to accept friend requests, therefore eliminating the commander's responsibility of friending and the perceptions that are attached to those relationships. Mullen's posts are innocuous, and he never responds directly to threads on his profile page.

To date there are no specific guidance for commanders and supervisors on setting up personal social network pages similar to Mullen's that negate the choice of friending. If Mullen had set up his Facebook page to accept "friends" he would be able to view the relationships of his followers in his virtual community, accessing over 16, 500 profiles that likely include private conversations, illicit photos, and possibly unprofessional relationships. How would having access to over 16,500 profiles have changed the dynamics of the relationships with Adm. Mullen? Although Mullen is passive on his own Facebook page, what level of responsibility does he and the DOD expect local commanders to maintain when they open a Facebook account? There are no guidelines for commanders on creating a social network profile. Should commanders remain passive and use their network account to share information only, or should commanders take an active role in ensuring the troops are not violating the current DOD policy on social network sites? Does the following excerpt from *Air Force Instruction 36-2909, Professional and Unprofessional Relationships,* apply to military supervisors and subordinates utilizing Facebook as the forum to communicate?

> The Air Force encourages personnel to communicate freely with their superiors regarding their careers, performance, duties and missions. This type of communication enhances morale and discipline and improves the operational environment while, at the same time, preserving proper respect for authority and focus on the mission.[26]

Personal relationships that are not initially unprofessional may become unprofessional when facts or circumstances change, and military experience has shown that certain types of relationships present a high risk of becoming unprofessional.[27] Take for example the noncommissioned officer (NCO) and the captain who like football. They are 'friends" on Facebook and their chosen football teams are rivals. The NCO and Captain make posts on

Facebook when the other team loses a game. Is this considered unprofessional communication? Later, the Captain and the NCO meet at the base club to watch their rival teams play while they both enjoy a few beers. Is this an indication of a change in their relationship? Next, the Captain decides to post pictures on Facebook of him and the NCO drinking beer while watching the game at the club. What message does this send to the Captain's subordinates? Per *AFI 36-2909*:

> While personal relationships between Air Force members are normally matters of individual choice and judgment, they become matters of official concern when they adversely affect or have the reasonable potential to adversely affect the Air Force by eroding morale, good order, discipline, respect for authority, unit cohesion or mission accomplishment. Military members understand that the needs of the institution will sometimes outweigh personal desires (Emphasis added).[28]

Clearly there is a need for education, but where does the military begin? Should the Pentagon have initiated relationship guidelines and training prior to allowing all soldiers to utilize social networking sites on the military's non-classified computer networks? The Air Force guidance, *AFI 36-2909*, on "shared activities" for social off-duty interests is a decade behind the times.

> *3.4. Shared Activities.* Sharing living accommodations, vacations, transportation, and off-duty interests on a frequent or recurring basis can be, or can reasonably be perceived to be, unprofessional. These types of arrangements often lead to claims of abuse of position or favoritism. It is often the frequency of these activities or the absence of any official purpose or organizational benefit which causes them to become, or to be perceived to be, unprofessional (Emphasis added). [29]

Social networking experts point out the advantage to connecting on-line with a current boss on Facebook is the opportunity for more personalized networking. When you connect on-line, users get to know one another better. Knowing one another better means discovering common interests that could help the boss know an employee better as a person. These personal connections can become major assets when you are looking to move forward in a career or to find a new job.[30] In a November 2010 article posted by the *Air Force Times*, "Airmen have to figure out for themselves when a cyberspace ’friend’ becomes something more.”Michelle McCluer, executive director at the National Institute of Military Justice at American University in Washington, goes on to say,

> “The Air Force’s lack of an online fraternization policy is probably because relationships are such a gray area. Fraternization is very much a sliding scale. But you could have a problem if you’re socializing as equals (referring to officers and enlisted). If I were still briefing people, I’d say not to friend your boss and not to friend your subordinates.”[31]

Without guidance, commanders must use discretion in determining the frequency of Facebook conversations, determining if there is an absence of any official purpose as part of the shared activity, and if having subordinates and supervisors “friending” each other on social networks is appropriate. According to Principal Deputy Assistant Secretary of Defense for Public Affairs Price Floyd, “What we (the DOD) can’t do is let security concerns trump doing business. We have to do business…We need to be everywhere men and women in uniform are and the public is. If that’s MySpace, and YouTube, that’s where we need to be, too.”[32]

First Amendment Rights. If the DOD and commanders are “virtually” everywhere with the troops and the public, what does this mean for the First Amendment rights of military members? The idea of the First Amendment to the Constitution is that Congress cannot make any laws limiting free speech. *Social Media and the Air Force* describes social networking policies in an attempt to explain what is acceptable and unacceptable behavior, however, social networking is new, and as negative outcomes impact mission effectiveness, new policies will evolve quickly. The military can punish soldiers for poor conduct, even when troops are not at work when posting comments or blogging.[33] The remaining concern for commanders is to what extent are they responsible in on-line communities, and will they be responsible when military members post appalling comments on commanders social network pages or other military members pages? Without clear guidance for commanders it will be difficult to outline how the owner of the social network page should be disciplined. Allowing negative postings on public sites, the owner of the page has enabled the action and should be held accountable. Network users are responsible for the information on their public sites, even electronic sites. A responsible social network user is one that checks their postings regularly and deletes anything questionable or deletes the person making inappropriate comments.[34]

Social Media and the Air Force recommends that social network users set privacy settings to “private” so that only ‘friends’ can see profile specifics.[35] What does this mean for local commanders’ who have ‘friends,’ are they responsible for routine monitoring of subordinates in the virtual community especially when commanders have direct access to subordinates profiles and conversations? Per the 1 May 1999 version of *AFI 36-2909:*

> Leadership requires the maturity and judgment to avoid relationships that undermine the respect for authority or impact negatively on morale, discipline, respect for authority, or mission of the Air Force. The senior member in the relationship is in the best position to appreciate the effect of that relationship on an organization and in the best position to terminate or limit the extent of the relationship.[36]

The First Amendment is not a guarantee of absolute free speech. A report by Dr. Andre Oboler points out that U.S. laws governing protected speech do not apply to private spaces such as Facebook, and it is up to Facebook to decide what to include and exclude from their privately owned website. The First Amendment does not force Facebook or anyone else to host content they consider objectionable. Libel and defamation are also not protected speech in the United States, but Facebook repeatedly defends certain conversations and pages on the basis of free speech. Simply being allowed to post unpleasant comments on Facebook does not mean it is a Constitutional right. There has been a public call for internet regulation, just as film, and computer games are regulated, and if companies such as Facebook abdicate that responsibility, advocates of internet regulation suggest government intervention.[37] Recommendations from an

Air Force legal office regarding Facebook explain that the First Amendment is not a blanket right for military members to do and say what they want at all times, especially in a global forum like the internet. The Supreme Court has long recognized that military members' First Amendment rights are limited due to the substantial and important need to preserve good order and discipline and to protect operational security.[38]

Social Networking on Duty. The Department of Defense allows access to social networking sites on government non-classified computers during duty time, yet 54% of U.S. civilian companies are prohibiting access to social sites while at work. An information technology research firm, Nucleus Research, conducted a study on employee productivity and the utilization of social networking sites while at work. The study concluded productivity drops 1.5% for companies that allow full access to Facebook in the workplace. In addition, the same study revealed of those using Facebook at work, 87% said they had no clear business reason for accessing the network.[39] To what extent are military personnel utilizing social sites for other than mission essential purposes and how has allowing access to social sites on government computers affected mission productivity? Additionally, human resource experts believe employers can be held liable for the actions of their employees who generate negative or offensive comments on social networking sites while on company computers during work hours.[40] The DOD can be held liable for comments made by their employees utilizing government computers during duty hours and making access available to hundreds of viewers across a rapid cyber spectrum. It will become the responsibility of local commanders to deal with complaints from victims of disparaging remarks on social networks when the comments were made during government time on government computers.

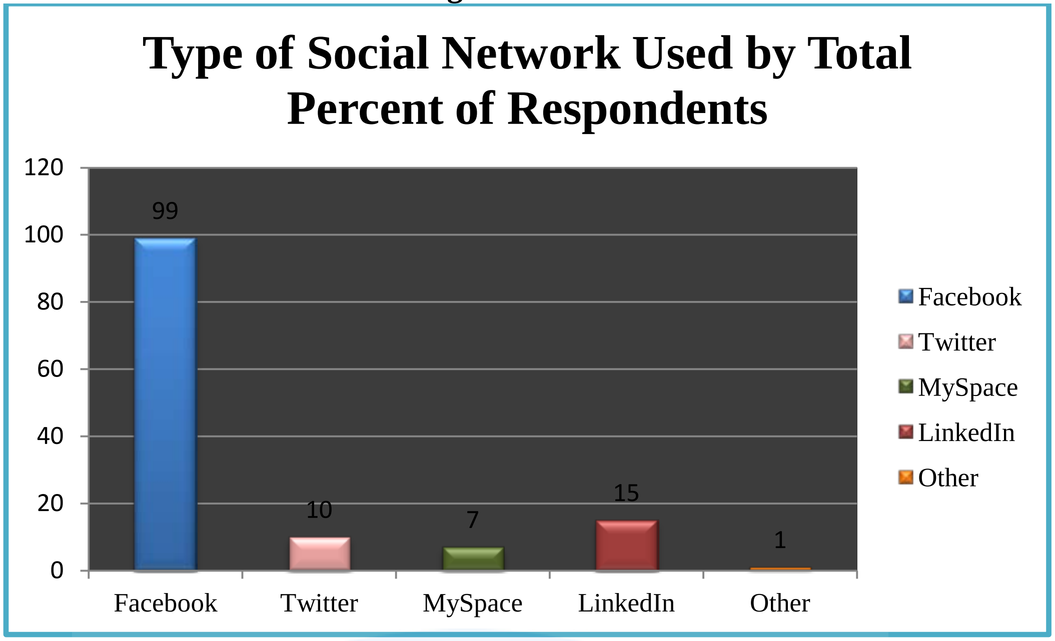
Methods: 2011 Survey Results

The following research was approved by the Maxwell Air Force Base Air University review board, and was conducted in accordance with the applicable Air Force Instructions. The survey was conducted with two generations of Air Force officers who have been part of the information technology revolution. The two groups selected were students from the Air and Space Basic Course (ASBC) and from the Air War College (AWC) at Maxwell Air Force Base, Alabama. A total of 348 ASBC students and 131 AWC students were given access to the survey. 111 lieutenants, 7 captains, and 47 lieutenant colonels/colonels for a total of 165 participants completed the survey. Not all participants answered each question, and aggregate data has been provided to delineate the results. The results will be provided for each of the seven questions. Free text was allowed for each question so that participants could expand on their responses.

Findings

Social Network Sites Used. (Figure 1**)**. For the total respondents, 99% use Facebook, 10% use Twitter, 7% use MySpace, 15% use LinkedIn, and 1% use another social network site. This is a clear indication of the growing use of social networking sites when compared to the Air Force social media use survey from 2008. Of the social networks available, 100% (N=111) of the lieutenants use Facebook, 100% (N= 7) of captains use Facebook, 36% (N=17) lieutenant colonels/colonels use Facebook, and 10.6% (N=5) of lieutenant colonels/colonels use LinkedIn. The remainder of the participants did not indicate the form of social networks utilized.

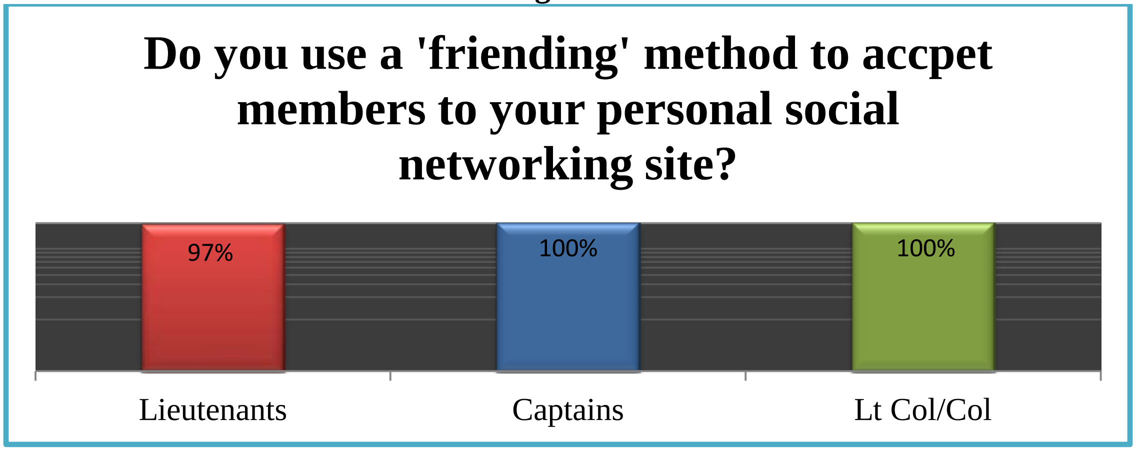
Figure 1.



Do you use a 'friending' method to accept members to your personal social networking site?

The lieutenants ranging in age from 22 to 30, indicated that 97% (N=108) use a friending method on their personal sites. The captains ranging in age from 26 to 37, indicated 100% (N=7) use a friending method (Figure 2). The lieutenant colonels/colonels ranging in age from 38 to 50, indicated 100% (N=19) use a friending method. The data provided is from respondents that actually indicated they use friending methods, not all respondents provided data for each question.

Figure 2.



For the lieutenants that do use a 'friending' method to accept individuals on their personal social network sites the responses were as follows:

- *"If I know them, I accept"*

- *"I only allow people to friend me if the person has a friend in common."*

- *"I accept all members who I know, all other requests are denied."*

The responses from the captains and lieutenant colonel/colonels were similar in their methods for "friending" on their personal websites. The responses from lieutenant colonels/colonels included:

- *"only if I actually know them"*

- *"people I know from personal contact"*

- *"I only accept friend requests from people that I personally know."*

Do you 'friend' military superiors on your personal social network site? The majority of respondents do not friend their superiors, with 54% of lieutenants, and 61% of lieutenant colonels/colonels opting to keep superiors out of their social network pages. The general reasons from all ranks to not friend a superior included:

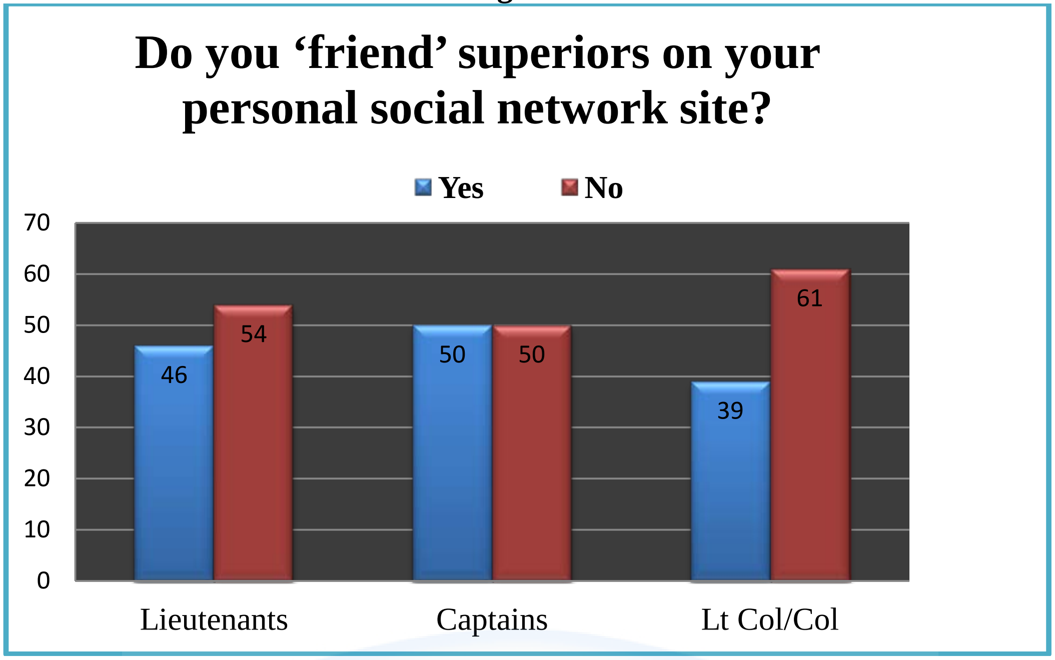
- *"I don't need my boss seeing all my personal information/photos."*

- *"I said no because I haven't yet, but I struggle with deciding if I will. It depends on how superior they are, the reasoning behind staying connected to them, and whether they are or may be in my chain of command."*

- *"I do not see the need to censor what my 'friends' write on my wall. I believe there should be a level of separation from what I do during my 'free' time and what I do in the workplace."*

- *"Normally I do not wish for military superiors to be continuously updated on my personal life just in case I post something they disagree with or find offensive."*

Figure 3.

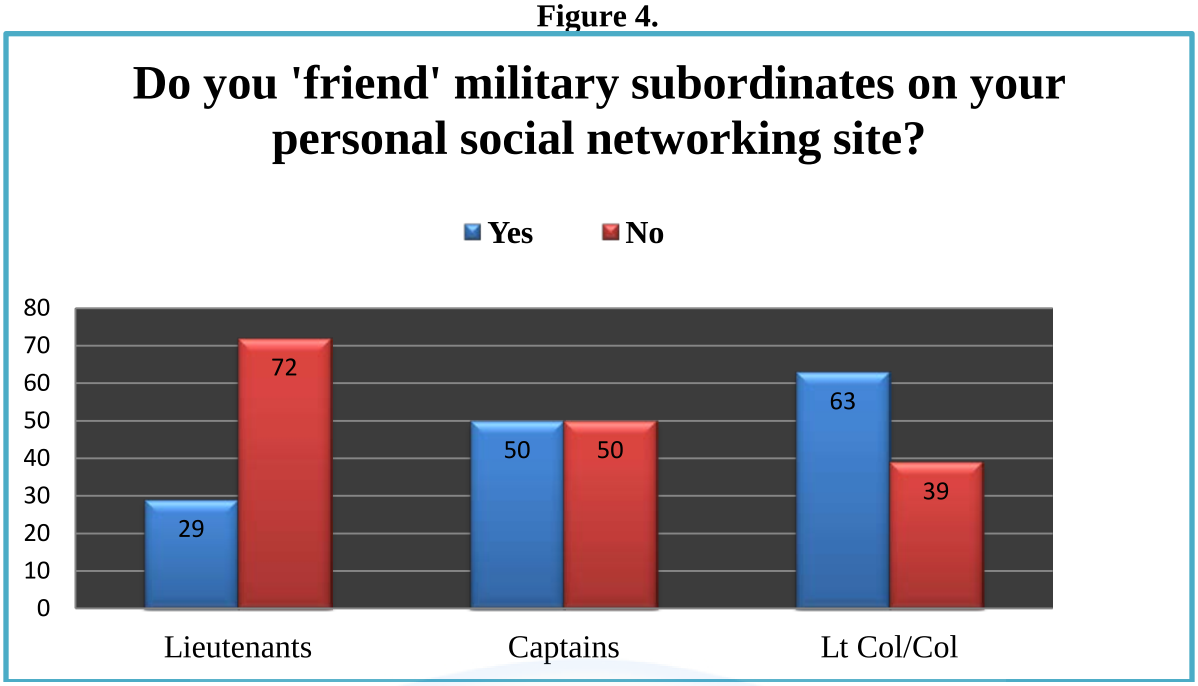


The survey indicates over 46% of lieutenants, 50% of captains, and 39% of lieutenant colonels/colonels friend their superiors (Figure 3). The general purpose all ranks provided for friending superiors was explained in free text as:

- *"For networking purposes."*
- *"Some of them I will. None of the officers in my direct chain of command are on Facebook and probably wouldn't know how to use it."*
- *"I friend military superiors however their rank and respect owed to them is always maintained, their friendship on these sites is only used as another form of communication and by no means a primary method."*

Do you 'friend' military subordinates on your personal social networking site? For the 140 total respondents that answered this question, the majority of lieutenants replied that they do not friend subordinates, while the majority of lieutenant colonels/colonels do friend subordinates (Figure 4). The findings for this question are significant as there are obvious disparities among the ranks.

Figure 4.



From the lieutenants who responded, the 72% that do not friend subordinates stated the following to explain their reasoning:

- *"Trying to remain professional."*
- *"I do not think people in your chain of command should be friends on Facebook."*
- *"I don't really have any military subordinates at this point in my career."*
- *"I do not want them (subordinates) checking out every aspect of my life."*
- *"I won't do it at all (friending subordinates) because I'm not sure they understand the difference between Facebook 'friends' and real friend."*
- *"There is personal information that not all subordinates need to know about."*

Of the lieutenant colonels/colonels, the 63% that do friend subordinates listed these reasons:

-*" They are people whom I have spent considerable time with in the past and I consider them friends that I want to keep in touch with.*

- *"To continue to mentor after PCS."*
- *"But only FORMER subordinates. As with supervisors, I consider many former*

subordinates to be friends."

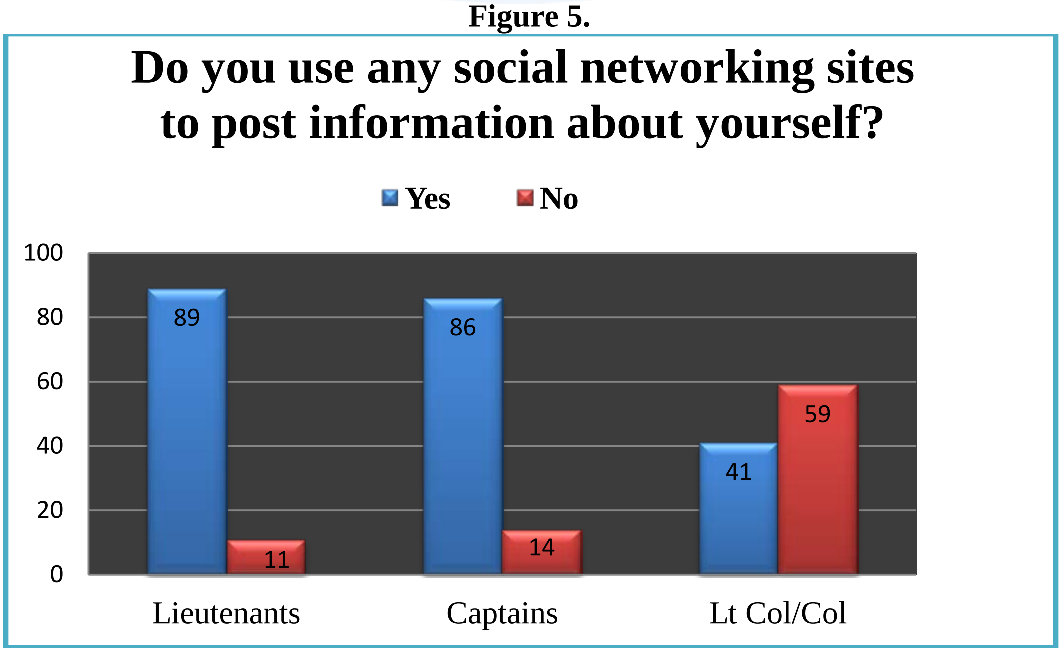
- *"Allows me to stay in contact with persons from my military career."*

Do you use privacy settings to restrict some information on your social networking site? A large percentage of all officer ranks utilize privacy settings, 96% (N=107) of lieutenants, 100% (N=7) of captains, and 100% (N=19) of lieutenant colonels/colonels. The majority of respondents provided reasons for setting privacy settings that included:

- *"Typically restrict most personal information and details from my public profile."*
- *"Only people who I know and accept are allowed to view more details."*
- *"I used privacy settings to prevent non 'friended' members from gaining potential access to information they could use against me."*
- *"I don't want my information to be out for everyone to see."*

Do you use any social networking sites to post information about yourself? Nearly 89% of the lieutenants and 86% of the captains utilize social networking sites to post information about themselves, while only 41% of lieutenant colonels/colonels utilize the social sites to post information about themselves (Figure 5).

Figure 5.



Sufficient military guidance has been issued to give me confidence I understand the behaviors appropriate for a USAF officer using social network sites? Respondents were asked to rate this question with strongly agree, agree, slightly agree, slightly disagree, disagree, and strongly disagree (Figure 6). Of the lieutenants that responded to this question 79% agreed in some form they have been given appropriate guidance, , 21% strongly agreed and 37% agreed.. Reasons given in free text by lieutenants were as follows:

- *"Plenty of briefings were given on basic protocol regarding what goes on social networking sites."*

- *"I feel that they (commissioning source) have taught me the boundaries between superiors and subordinates and what is becoming of an officer."*

- *"While no specific guidance has been issued, there are hints that have been dropped."*

- *"I have received guidance only when someone does something wrong, never prior to that."*

- *"I have received several updates and guidance through unit e-mails that have aided me in better understanding social media."*

Smaller numbers of lieutenant colonels/colonels from the respondents stated their guidance was sufficient. 62% agreed in some form they had received sufficient guidance, 23% slightly agreed and 11% strongly agreed. Listed below is a representative sample from the responses of the 36% of lieutenant colonels/colonels that disagree to some extent on receiving adequate guidance that provides confidence in understanding the behaviors expected of USAF officers that utilize social network sites:

- *"I have been in the military long enough to understand what is appropriate to post on networking sites, even with privacy settings enabled. But I don't think enough guidance has been given for young officers who have been using these sites for years to communicate all of their activities, opinions, and feelings to their friends"*

- *"The training included in Information Assurance CBTs (computer based tests) is not sufficient to clarify all of the methods and settings for different user programs. It* *would behoove the AF to take a proactive stance on social networking and create, update and PUSH-to-publish 'Security Tips' for personal users as well as professional users. The only current guidance is PULL-to-access from the AF Portal"*

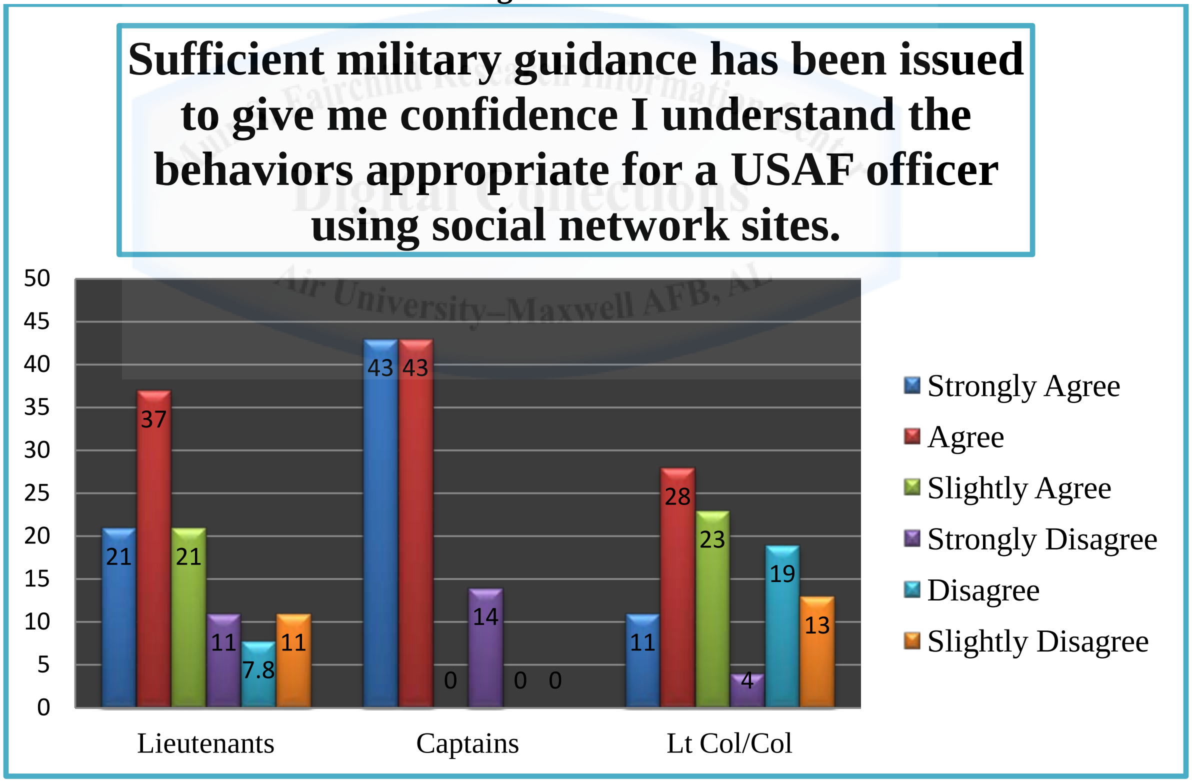
- *"I've heard some suggestions in a hap hazard manner but have not received adequate 'issued guidance'"*

- *"There is a hazy issue over what could be interpreted as violations of articles of the UCMJ regarding use of social media. As a commander this troubles me"*

- *"While I'm aware that members can access various sites, I have no idea what to do with them (social network sites) or how to use them"*

- *"I may not have seen it (guidance) because I don't use them (social network sites), however, I've not seen any specific guidance on the use of these networks on gov't computers."*

Figure 6.



Research Implications

From the cumulative data collected on this topic, this research has identified a need for more detailed guidance for commanders and subordinates on utilizing social networks. This includes rules for “friending” between superiors and subordinates, reading the user agreement statements for social network sites, and the level of responsibility for commanders who have access to the personal postings of subordinates.

Friending Implications. It can be assumed these groups of ASBC and AWC students are friending individuals related to the social norms of endorsing that person as a close contact with trust and not on the perception is friending is simply a system descriptor, and this description does not necessarily imply a close relationship. Will this mean a slippery slope for professional relationships on social networking sites utilized by our armed forces?

A very clear distinction was made for lieutenant colonels/colonels, the majority of whom friend subordinates on their personal social network sites, yet only 39% report friending superiors. The lieutenant colonels/colonels that chose to friend subordinates related this practice to mentoring, keeping in touch, and for personal relationships. Many also stated them only friend subordinates after they are no longer their commander or have changed duty stations; however, none of the responses listed the possibility of being assigned again with the same subordinate and how that relationship would be affected. Lieutenants do not friend subordinates and supervisors equally. Lieutenants stressed keeping their personal life personal and keeping professional relationships in perspective whether it is with subordinates or supervisors.

The data demonstrates lieutenant colonels/colonels want to share information with subordinates through social network sites, but emphasis should be placed on the interpretation of those relationships and ensuring those relationships are maintained in a professional forum to eliminate the misinterpretations of social networking communications. What are the implications and risks associated with the friending practices of senior ranking officers with subordinates, especially when the military lacks explicit guidance?

Privacy Implications. From this small group of respondents, military members are under the impression that if they use privacy settings to restrict information on their social networking sites their personal information is protected. However, Facebook clearly states their limited privacy guarantees in their user agreements. The survey question related to posting personal information on social networks did not allow for free text for respondents to elaborate on their answers on posting personal information. In order to determine why respondents utilize social networks to post personal information, a free text response could have strengthened this survey question. What are the implications for the 63% of lieutenant colonels/colonels that "friend" the 89% of subordinates that post personal information on their sites? Are commanders required to police these sites in the same way civilian employers police these sites to identify discriminating information?

Guidance Implications. It is concerning that of the lieutenants, 79% feel they have received enough guidance, while less than 62% of lieutenant colonels/colonels feel they have received sufficient guidance to utilize social network sites and feel confident enough to understand the behaviors appropriate for officers using the sites. The comments provided by senior officers who feel they have not received enough guidance clearly indicate a need for more defined expectations and standardized training. What implications will this lack of confidence from commanders and future commanders have on facilitating education for those they command?

Proposed Guidance & Consequences

The bottom line comes from the *Joint Publication 1-0*, "Information is an instrument of national power and has complex components with no single center of control."[41] This makes the task of policing social network societies a daunting challenge for commanders. The Air Force should start by updating *AFI 36-2909, Professional and Unprofessional Relationships,* to reflect the responsibilities of its members in the cyber domain, and provide guidance for commanders that participate in virtual networks with subordinates. The instruction needs a complete section dedicated to guidelines for on-line social network behavior. The guidance and consequences contained herein are "proposed" and the ultimate responsibility for ensuring effective, efficient, and appropriate use of internet-based capabilities lies with the individual military member. Anytime a soldier, sailor, or airman engages in social media, they are representing their service, and therefore should not do anything that would discredit themselves or the service they represent.[42]

The following are suggested guidelines for *AFI 36-2909*:

1. Military commanders reserve the right to view a military member's public social network sites when those sites are accessed on government computers during government working hours.

2. Monitoring personal network pages is the responsibility of the military member. Unprofessional postings by others on military members' pages may reflect poorly on the military and the member. Members should block postings from individuals who post unprofessional content.

3. All content associated with users of social networking sites should be consistent with the values and professional standards set forth by the United States Air Force. This includes photographs, videos, membership in groups, demographic information, and posted statements/comments.

4. Military members are responsible for reporting unprofessional comments, photos, videos, or group memberships by DOD employees to their respective chain of command.

5. Military members are responsible for monitoring the social network privacy and security settings regularly, and ensuring they have read and understand the network user agreement terms before establishing a user account.

6. Military members are responsible for ensuring photos that are "tagged" of them in social network sites are appropriate and are not compromising to the individual member or to the military. Military members are responsible to "untag" themselves

from inappropriate photos, and to refrain from tagging others unless they have explicit permission to do so.

7. Military members are not to have interactions with subordinates they directly supervise unless it is specifically mission related. Interactions other than mission related provides an opportunity for a dual relationship, which may inadvertently disrupt good order and morale. In addition interactions with subordinates on social network sites can lead to real and perceived unprofessional relations.

8. Commanders may create a local social networking homepage for interactions between supervisors and subordinates. The commander retains the responsibility for monitoring and maintaining the local site. The commander must make public the availability of the site to all members of the unit, and ensure all members of the unit have equal opportunity to access the site.

9. It is the responsibility of commanders and supervisors at all levels to ensure the fundamental expectation and adherence to customs/courtesies and maintenance of professional relationships in all environments, both physical and virtual. Commanders and supervisors must stress “knowing your audience” when laying down the rules of engagement for social networking sites, communicate the various perceptions on social sites and how they can disrupt good order and morale if misinterpreted, clarify the perceptions of unprofessional relationships as it pertains to supervisors/subordinates or officers/enlisted.

In addition to guidelines, *AFI 36-2909* should outline consequences of unprofessional behavior on social network sites in particular that include:

1. Postings made by military members on social networking sites may be subject to the *Uniformed Code of Military Justice (UCMJ)* and virtual interactions on social networking services, social media, user-generated content, social software, and discussion forums are subject to the same standards of professionalism as face-to-face interactions between military members.

2. Use of social networking sites can have legal ramifications, and information posted on these sites may be used in disciplinary measures and/or for *UCMJ* purposes.

3. Participants in social networking sites may be called upon as witnesses in disciplinary actions regarding military members.

4. In addition to *UCMJ* actions, military members may be subject to punishment under the *Privacy Act of 1974, Public Law 93-579,* for violations of personal privacy and security.

Conclusion

Maintaining a presence in the cyber domain is both necessary and valuable as a strategic resource and vital to national security allowing communicators to shape the information battlefield.[43] According to the *Pew Research Center,* online social activity is highest among teens and young adults with nearly 72% of young adults and teens using social network sites compared to 40% of adults 30 and older. The study also reveals younger people tend to be more digitally savvy and socially connected online.[44] The revolution of Web 2.0 social networking has created challenges for commanders and supervisors in friending, deciphering content, privacy, professional and unprofessional relationships, First Amendment rights, and social networking on duty. Proposing more detailed regulations on Internet-based capabilities, the Air Force recently updated *AFI 33-100, User Responsibilities and Guidance for Information Systems*, and *AFI 33-129, Web Management and Internet Use*. While the author of this paper recognizes the risks of malicious activity and cyber attack in virtual societies, the risks of unprofessional relationships that degrade effective military operations has been overlooked in the cyber society. There are several areas still not addressed by current Air Force instructions, to include: professional and unprofessional internet relationships, specifics for commanders on maintaining content and security of information posted on public/private websites, as well as guidance for commanders and supervisors with information technology settings on personal network pages to avoid the pitfalls of friending. David Kilcullen, *Fundamentals of Company Level Insurgency*, aptly describes information wars “in this battlefield, popular perceptions and rumor are more influential than facts and more powerful than a hundred tanks.”[45] More explicit cyber tactics, techniques and procedures for those in positions of leadership regarding the openness and transparency with online audiences are needed to ensure good order and discipline and prevent misinterpretations of relationships. The guidance thus far provided by the DOD and the Air Force has been limited and incomplete. More solid directions on the appropriate use of social networking sites addressing the challenges faced by commanders is greatly needed and hopefully forthcoming or the bedrock of military professionalism may be called into question.

[1] Jelinek, P. "Pentagon changes policy, allows all soldiers to use Twitter, Facebook." www.huffingtonpost.com/2010/02/26/pentagon-changes-rule-all_n_479211.html

[2] Miles, D. "Military Leaders Embrace Facebook, Twitter, My Space" www.af.mil/news/story.asp?id=123158264

[3] *At War.* October 3, 2009. http://atwar.blogs.nytimes.com/2009/10/13/military-web-policy

[4] United States Air Force. "Social Media and the Air Force" p. 14-15.

[5] Ibid, p. 14.

[6] Ibid, p. 7.

[7] Boyd, D.M. "Social network sites: definitions, history and scholarship." www.jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

[8] Jelinek, P. "Pentagon changes policy, allows all soldiers to use Twitter, Facebook."

[9] Boyd, D.M. "Social network sites: definitions, history and scholarship." *jcmc.indiana.edu.* 2007. jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

[10] Ibid.

[11] Ibid.

[12] Fono, D., and K. Rayes-Goldie. "Hyperfriendship and beyond" *Internet Research Annual Volume 4*, 2006: 91-103.

[13] Ibid.

[14] Ibid.

[15] The Judge Advocate General's School. *Military Commander and the Law*, p. 221-223

[16] Ibid.

[17] Appel, Ed. *Social Media the Internet and Law Enforcement: Cybervetting and Posting.* January 10, 2011. www.inamecheck.com.

[18] *Ibid.*

[19] *Ibid.*

[20] Baron, Kevin. "Watchdog group: Dozens of active-duty found on neo-Nazi site." *www.stripes.com.* July 10, 2009. http://www.stripes.com/news/watchdog-group-dozens-of-active-duty-troops-found-on-neo-nazi-site-1.93224

[21] Facebook. *Facebook's Privacy Policy.* December 22, 2010. http://www.facebook.com/policy.php

[22] Randall, David, and Victoria Richards. "Facebook Can Ruin Your Life." *The Independent.* http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-can-ruin-your-life.

[23] Hastings, Michael. *Another Runaway General: Army Deploys Psy-Ops on U.S. Senators.* February 23, 2011. http://www.rollingstone.com/politics/news/another-runaway-general-army-deploys-psy-ops-on-u-s-senators-20110223

[24] *Ibid.*

[25] McMichael, W. "DoD may curb Facebook and Twitter access." http://infoweb.newsbank.com/iw-search/we/InfoWeb

[26] *AFI 36-2909.* "Professional and Unprofessional Relationships." p. 3

[27] Powers, Rod. "About.com: U.S. Military." *About.com.* 2010. http://usmilitary.about.com/library/milinfo/afreg/blafi36-2909.htm

[28] *AFI 36-2909.* "Professional and Unprofessional Relationships." p. 3

[29] Ibid, p. 2

[30] Balderrama, A. "Should your boss be your facebook friend?" *CNN.com.* 2009. www.cnn.com/2009/LIVING/worklife/01/28/cb.facebook.boss.friend/index.html

[31] Fontaine, Scott. *Air Force Times "Facebook: Fraternization or a useful tool?".* Nov 22, 2010. http://www.airforcetimes.com/news/2010/11/air-force-facebook-useful-or-fraternization- 112110w/

[32] Shachtman, Noah. "Marines Ban Twitter, MySpace, Facebook." *Wired.com.* Aug 3, 2009. http://www.wired.com/dangerroom/2009/08/marines-ban-twitter-myspace-facebook/#ixzz12otLYqrR

[33] United States Air Force. "Social Media and the Air Force."

[34] Carpenter, E. S. "Free speech and social networking sites-the employment issue." *Examiner.com.* July 29, 2010. http://www.examiner.com/human-resources-in-jackson/free-s...-networking-sites-the-employment-issue?

[35] United States Air Force. "Social Media and the Air Force."

[36] *AFI 36-2909.* "Professional and Unprofessional Relationships." p. 3

[37] Martin, Caitlyn. "Report: Facebook A Haven for Hate Groups." *Broadcast.oreilly.com.* Sept 17, 2009. http://broadcast.oreilly.com/print/37968.html

[38] Ibarra, Cristobal. "So, you think Facebook, MySpace, and Twitter are just for fun and games? Think again." *www.af.mil.* Aug 19, 2010. www.af.mil/news/story_print.asp?id=123218487

[39] Gaudin, Sharon. *Study: 54% of companies ban Facebook, Twitter at work.* http://www.computerworld.com/s/article/print/9139020/Study_54_of_companies_ban_Facebook_Twitter_at_ work

[40] Gilhooley, Diane. *Accessing social-networking sites at work-a note of caution.* http://www.timeshighereducation.co.uk/story.asp?storyCode=406048&sectioncode=26

[41] "Joint Publication 1." *Doctrine for the Armed Forces of the United States.*

[42] United States Air Force. "Social Media and the Air Force" p. 7.

[43] Ibid, p. 2.

[44] Porterfield, Amy. *Social Media Use Among Teens, Boomers and Moms: New Studies Reveal Great Insight.* March 5, 2010. http://www.socialmediaexaminer.com/social-media-differences-among-teens-boomers-and-moms-new-study-findings/

[45] United States Air Force. "Social Media and the Air Force" p. 14. This quote by David Kilcullen was in the USAF public affairs publication social media stressing the importance of info wars.

Bibliography

AFI 36-2909. "Professional and Unprofessional Relationships." HQ USAF, May 1, 1999. "At War." *At War.* October 3, 2009. http://atwar.blogs.nytimes.com/2009/10/13/military-web-policy (accessed October 28, 2010).

Appel, Ed. *Social Media the Internet and Law Enforcement: Cybervetting and Posting.* January 10, 2011. www.inamecheck.com (accessed March 30, 2011).

Balderrama, A. "Should your boss be your facebook friend?" *CNN.com.* 2009. www.cnn.com/2009/LIVING/worklife/01/28/cb.facebook.boss.friend/index.html (accessed August 26, 2010).

Baron, Kevin. "Watchdog group: Dozens of active-duty found on neo-Nazi site." *www.stripes.com.* July 10, 2009. http://www.stripes.com/news/watchdog-group-dozens-of-active-duty-troops-found-on-neo-nazi-site-1.93224 (accessed Nov 14, 2010).

Boyd, D.M. "Social network sites: definitions, history and scholarship." *jcmc.indiana.edu.* 2007. jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (accessed August 27, 2010).

Carpenter, E. S. "Free speech and social networking sites-the employment issue." *Examiner.com.* July 29, 2010. http://www.examiner.com/human-resources-in-jackson/free-s...-networking-sites-the-employment-issue? (accessed Nov 17, 2010).

Donath, J., and D. Boyd. "Public displays of connection." *BT Technology Journal* 22, no. 4 (2004): 71-82.

Facebook. *Facebook's Privacy Policy.* December 22, 2010. http://www.facebook.com/policy.php (accessed March 30, 2011).

Fono, D., and K. Rayes-Goldie. "Hyperfriendship and beyond: Friends and social norms onLiveJournal." *Internet Research Annual Volume 4*, 2006: 91-103.

Fontaine, Scott. *Air Force Times "Facebook: Fraternization or a useful tool?".* Nov 22, 2010. http://www.airforcetimes.com/news/2010/11/air-force-facebook-useful-or-fraternization-112110w/ (accessed Nov 23, 2010).

Gaudin, Sharon. *Study: 54% of companies ban Facebook, Twitter at work.* October 6, 2009. http://www.computerworld.com/s/article/print/9139020/Study_54_of_companies_ban_Fa cebook_Twitter_at_ work (accessed March 24, 2011).

Gilhooley, Diane. *Accessing social-networking sites at work-a note of caution.* April 1, 2009. http://www.timeshighereducation.co.uk/story.asp?storyCode=406048&sectioncode=26 (accessed March 24, 2011).

Hastings, Michael. *Another Runaway General: Army Deploys Psy-Ops on U.S. Senators* February 23, 2011. http://www.rollingstone.com/politics/news/another-runaway-general-army-deploys-psy-ops-on-u-s-senators-20110223 (accessed March 30, 2011).

Ibarra, Cristobal. "So, you think Facebook, MySpace, and Twitter are just for fun and games? Think again." *www.af.mil.* Aug 19, 2010. www.af.mil/news/story_print.asp?id=123218487 (accessed Nov 2010, 2010).

Jelinek, P. "Pentagon changes policy, allows all soldiers to use Twitter, Facebook." *Huffingpost.com.* Feb 26, 2010. www.huffingtonpost.com/2010/02/26/pentagon-changes-rule-all_n_479211.html (accessed August 27, 2010).

"Joint Publication 1." *Doctrine for the Armed Forces of the United States.* Washington D.C.: Department of Defense, March 20, 2009.

Martin, Caitlyn. "Report: Facebook A Haven for Hate Groups." *Broadcast.oreilly.com.* Sept 17, 2009. http://broadcast.oreilly.com/print/37968.html (accessed Nov 17, 2010).

McMichael, W. "DoD may curb Facebook and Twitter access." *NewsBank.* August 10, 2009. http://infoweb.newsbank.com/iw-search/we/InfoWeb (accessed August 26, 2010).

Miles, D. "Military leaders embrace Facebook, Twitter, My Space." *News, Interviews and More.* July 7, 2009. www.af.mil/news/story.asp?id=123158264 (accessed August 27, 2010).

Porterfield, Amy. *Social Media Use Among Teens, Boomers and Moms: New Studies Reveal Great Insight.* March 5, 2010. http://www.socialmediaexaminer.com/social-media-differences-among-teens-boomers-and-moms-new-study-findings/ (accessed March 17, 2011).

Powers, Rod. "About.com: U.S. Military." *About.com.* 2010. http://usmilitary.about.com/library/milinfo/afreg/blafi36-2909.htm (accessed Oct 19, 2010).

Randall, David, and Victoria Richards. "Facebook Can Ruin Your Life." *The Independent.* Feb 10, 2008. http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-can-ruin-your-life. (accessed Nov 13, 2010).

Shachtman, Noah. "Marines Ban Twitter, MySpace, Facebook." *Wired.com.* Aug 3, 2009. http://www.wired.com/dangerroom/2009/08/marines-ban-twitter-myspace-facebook/#ixzz12otLYqrR (accessed 10 28, 2010).

The Judge Advocate General's School. *Military Commander and the Law.* Maxwell Air Force Base: The Judge Advocate General's School, 2008.

Force, United States Air. "Social Media and the Air Force." Headquarters United States Air Force, 2010.